Town of Rockport

Acceptable Use Policy

(Network, Computer, Internet, & E-mail)

Adopted December 5, 2006

This Acceptable Use Policy (AUP) applies specifically to Town Hall, the Police Department, the Public Library, Fire Services, the Harbormaster's Office, the Council on Aging, and the Parking Clerk. Other policies apply for the Rockport Public Schools.

Computer and Electronic Communication Systems Policy

Purpose: The purpose of this policy (hereafter known as the "Policy") is to establish policies and provisions for all persons using any portion of Rockport's entire computer network, including, but not limited to: host computers, file servers, application servers, communication servers, mail servers, facsimile servers, web servers, work stations, stand-alone computers, laptops, software, data files and all internal and external computer and communications networks (such as the Internet, commercial online services, value-added networks, and E-mail systems) that may be accessed directly or indirectly from Rockport's computer network (hereafter known collectively as "Technology Resources").

Applicability: This policy is applicable to all Rockport departments, employees, and volunteers whether full-time, part-time, regular, or temporary, and to all consultants, independent contractors, temporary workers, and agents utilizing Rockport's Technology Resources (hereafter known collectively as "Users").

Responsibility: The Information Technology Department is responsible for the maintenance of this policy and for the education of Rockport employees regarding this policy. Rockport department managers and supervisors and the IT Department are responsible for monitoring compliance with this policy. It is every User's duty to use Rockport's Technology Resources responsibly, professionally, ethically, and lawfully.

POLICIES AND PROCEDURES

A. Communication of Policy

All Users are required to read and familiarize themselves with the Policy, and are further required to sign a written statement acknowledging that they have read and understand the Policy. All Rockport managers should work within their departments to ensure that all Users are aware of, understand, and follow the Policy guidelines. In addition, the Policy will be communicated to all new Rockport Users at the time of hire (or in the case of non-Rockport employees, before the time that the use of any Technology Resources commences). As is the case with all Rockport policies, the Town reserves the right to amend the Policy at any time without prior notice.

B. Use of Technology Resources

Technology Resources are the property of the Town of Rockport and are provided solely for legitimate operational purposes. Users are permitted access to the Town's Technology Resources to assist them in performance of their job functions. Use of Rockport Technology Resources is a privilege that may be revoked at any time. Therefore, Users shall limit their "personal" use of the Town's Technology Resources to lunch or during break periods. Technology Resources shall not be used for social interaction or personal entertainment. The determination of whether inappropriate use of Technology Resources has occurred will be handled on a case-by-case basis.

1. **E-mail Content.** All E-mail communications are to be treated with the same seriousness, courtesy, and formality as any other business communication. Users must take every precaution to draft all E-mail messages with the same care with which they would draft any other business document. Important communications or files should be stored in a safe and secure network directory and all other non-essential E-mail should be deleted after 30 days. As a public record, E-mail correspondence is subject to all the strictures of MGI, Ch 4, sec 7 (26).

2. **Restricted Access to the Internet.** To ensure security and avoid the spread of viruses, Users accessing the Internet through a computer attached to Rockport's network must do so through the approved Internet firewall. Accessing the Internet directly by modem is strictly prohibited unless you have obtained prior written approval from the IT Director (in this case, the computer will be disconnected from the Town's networks). Access to the Internet, news groups, mailing lists, and chat rooms requires prior approval from the IT department. Users may only utilize the web browser and E-mail software provided by the IT Department. Users may not access the Internet through their own Internet Service Provider (ISP).

3. **Data Retention.** All important business related data files should be stored in a safe and secure network location. Users understand that any data stored on their desktop computer, laptop, or otherwise "personal" workstation is not backed-up by the IT Department as normal operating procedure. Therefore, if Users choose to store data on their workstation they assume back-up responsibilities for that particular data. It is the Users responsibility to ensure that their data is stored in a safe, secure, and regularly backed-up location.

C. Privacy

1. **No Expectation of Privacy.** The computers and computer accounts provided to Users are to assist them in performance of their jobs. Users should not have an expectation of privacy in anything they create, modify, store, send, or receive on the Rockport computer system, including all E-mail messages.

2. **Waiver of Privacy / Consent to Monitor.** Users expressly waive any right of privacy in anything they create, modify, store, send, or receive on the computer, through the Internet, or any other component of the Town's network. Users consent to allowing authorized Rockport personnel to access and review all material created, modified, stored, sent, or received on the computer, through the Internet, or any other component of the Town's network, by either human or automated means and in a manner consistent with applicable state and federal law. Such access and review by authorized Rockport personnel can be done without prior notice to Users and is permitted in order to protect Rockport's legitimate operational interests. Users understand that system security features such as passwords and the Users ability to delete messages does not defeat the ability of authorized Rockport personnel to access and review any material.

D. **Prohibited Activities**

1. **Inappropriate or Unlawful Material.** Material that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory, or otherwise unlawful or inappropriate may not be sent by E-mail or other form of electronic communication (such as bulletin board systems, newsgroups, and chat groups) or displayed odor stored in Rockport computers. Users encountering or receiving any such material should immediately report the incident to their supervisor or manager who, in turn, should then report such incidents to Rockport's IT Director.

2. **Prohibited Uses.** Without prior written permission from the User's department manager or supervisor, and expressed approval from Rockport's IT Director, Technology Resources may not be used to disseminate or store commercial or personal advertisements, solicitations, promotions, destructive programs (viruses or self replicating code), political propaganda, or any other unauthorized use.

3. **Waste of Technology Resources.** Users may not deliberately perform acts that waste Technology Resources or unfairly monopolize resources to the exclusion of others. These acts include, but are not limited to, sending mass mailings or chain letters, spending excessive amounts of time on the Internet, downloading extraordinarily large files, playing games, engaging in online chat groups, printing multiple copies of lengthy documents, or otherwise creating unnecessary network traffic.

4. **Sending Unsolicited E-mail ("spamming').** Without the express permission from the User's manager or supervisor, Users may not send unsolicited E-mail messages to persons with whom they have not had a prior business relationship.

5. **Hiding Identity of E-mail Authors ("spoofing').** Users may not, under any circumstances, use spoofing or other means to disguise their identities in sending e-mails.

6. **Misuse of Software.** Software can only be used in compliance with the terms of applicable license agreements. Users understand that all applicable state and federal copyright laws apply to the use of software applications.

All applications (including programs, screen savers, etc.) running on Rockport Technology Resources must be pre-approved by the IT Department and can only be installed by qualified IT Department staff. Installation of any non-business related applications (i.e., AIM, AOL, games, stock tickers, horoscopes, web shots, etc.) is expressly prohibited by Town policy. Employees should not purchase, download, or install any application without first receiving permission from their manager or supervisor, and then obtaining written approval from Rockport's IT Director.

Without prior written permission from Rockport's IT Director, Users may not do any of the following: (1) copy software for use on their home computers; (2) provide copies of software to any non-Rockport employee; (3) install any software on any of Rockport's PCs, workstations, or servers; (4) download any software from the Internet or other online service to any of Rockport's PCs, workstations, or servers; (5) modify, revise, transform, recast, or adapt any software; or (6) reverse-engineer, disassemble, or decompile any software.

Users who become aware of any misuse of software or violations of copyright law should immediately report such incidents to their manager or supervisor who, in turn, should report such incidents to the IT Director.

7. **Personal Use.** Technology resources are for legitimate operational purposes only and personal use within the above parameters is limited to lunch or other break periods.

E. Passwords

1. **Responsibility for Passwords.** Users are responsible for safeguarding their passwords for access to the computer system. Individual passwords should not be printed, stored online, or given to others. Users are responsible for all transactions made using their passwords. No User may access the computer system with another User's password or account.

2. **Passwords Do Not Imply Privacy.** Use of passwords to gain access to the computer system or to encode particular files or messages does not imply that Users have an expectation of privacy in the material they create or receive in the computer system. Rockport utilizes global passwords that permit access to all material stored on its computer system, regardless of whether that material has been encoded with a particular User's password.

F. Security

1. **Accessing Other User's files.** Users may not alter or copy a file belonging to another User without first obtaining permission from the owner of the file. Ability to read, alter, or copy a file belonging to another User does not imply permission to read, alter, or copy that file. Users may not use the computer system to "snoop" or pry into the affairs of other Users by unnecessarily reviewing their files and E-mail.

2. **Accessing Other Computers and Networks.** A User's ability to connect to other computer systems through the network or by a modem does not imply a right to connect to those systems or to make use of those systems unless specifically authorized by the operators of those systems.

3. **Computer Security.** Each User is responsible for ensuring that use of outside computers and networks, such as the Internet, does not compromise the security of Rockport's Technology Resources. This duty includes taking reasonable precautions to prevent intruders from accessing the company's network without authorization and to prevent introduction and spread of viruses.

G. Viruses

Viruses can cause substantial damage to the Town's network and computer systems. The Town is safeguarded against such threat with network and workstation anti-virus protection. Even so, each User is still responsible for taking reasonable precautions to ensure he or she does not introduce viruses into the Rockport network.

To that end, all material received on floppy disk, or other magnetic or optical medium, and all material downloaded from the Internet, or from computers or networks that do not belong to Rockport MUST be scanned for viruses and other destructive programs before being placed into the computer system.

Users should understand that their home computers and laptops may contain viruses. All disks and files transferred from these computers to Rockport's network MUST be scanned for viruses.

G. Encryption Software

1. **Use of encryption software.** Users may not install or use encryption software on any of Rockport's computers without first obtaining written permission from Rockport's IT Director. In addition, Users may not use passwords or encryption keys that are unknown to the Information Technology Department.

2. **Export restrictions.** The federal government has imposed restrictions on exports of programs or files containing encryption technology (such *as E-mail* programs that permit encryption of messages and electronic commerce software that encodes transactions). Software containing encryption technology is not to be placed on the Internet or transmitted in any way outside of the United States without prior permission from Rockport's IT Director.

I. Miscellaneous

1. **Disclaimer of Liability for use of Internet.** The Town of Rockport is not responsible for material viewed or downloaded by Users from the Internet. The Internet is a worldwide network of computers that contains billions of pages of information. Users are cautioned that many of these pages include offensive, sexually explicit, and inappropriate material. In general, it is difficult to avoid at least some contact with this material while using the Internet. Even innocuous search requests may lead to sites with highly offensive content. In addition, having an E-mail address on the Internet may lead to receipt of unsolicited E-mail containing offensive content. Users accessing the Internet do so at their own risk.

2. **Attorney-Client Communications.** E-mail communications sent to and from Town Counsel or any other attorney representing the Town should include this warning header on each page: "ATTORNEY-CLIENT PRIVILEGED; DO NOT FORWARD WITHOUT PERMISSION"

3. **Compliance with Applicable Laws and Licenses.** In their use of Technology Resources, Users must comply with all software licenses, copyrights, and "all" other state, federal, and international laws governing intellectual property and online activities.

4. **Amendments and Revisions.** This Policy may be amended or revised from time to time as the need arises. Users will be provided with copies of all amendments and revisions.

5. **No Additional Rights.** This Policy is not intended to, and does not grant Users any contractual rights.

J. Disciplinary Actions

Failure To Comply With This Policy. All Users are required to comply with this Policy. Violations of this Policy may be grounds for disciplinary action, up to and including termination of employment where appropriate. In the event of any contradiction between this Policy and any statement made by a Rockport employee with managerial or supervisory authority, the provisions of this Policy govern.

Town of Rockport
Acceptable Use Policy Highlights

DO:

- Use technology resources for business purposes
- Limit any "personal" use of Town owned technology resources to break periods
- Use only the Town provided Internet connection and software
- Use e-mail in a professional manner to better serve our customers
- Draft e-mail with the same seriousness as any other business document
- Delete non-essential e-mail after 30 days
- Store important e-mail and files in a safe and secure directory
- Safeguard your password to ensure security of the network
- Be aware that your data is not private and may be used as evidence
- Scan floppy disks, magnetic media, and optical disks for viruses before accessing data

DON'T:

- Use technology resources for social interaction and personal entertainment
- Use inappropriate, offensive, or defamatory language in electronic correspondence
- Access news groups, outside bulletin boards, mailing lists, or chat rooms
- Install or download any software, executable files, or screensavers, etc.
- Access or make unauthorized changes to other users files or directories
- Include sensitive medical or private information in e-mail correspondence
- Access large media files (video or audio) that use up bandwidth capacity
- Use outside e-mail services for business correspondence

Town of Rockport

Acceptable Use Policy

(Network, Computer, Internet, & E-mail)

This Acceptable Use Policy (AUP) applies specifically to Town Hall, the Police Department, the Public Library, Fire Services, the Harbormaster's Office, the Council on Aging, and the Parking Clerk. Other policies apply for the Rockport Public Schools.

I have read, understand, and agree to comply with the terms of this Policy governing use of Rockport's Technology Resources. I understand that a violation of this Policy may result in disciplinary action, up to and including termination of employment, as well as civil or criminal liability.

_____ Date: _____

User's Signature

_____

User's Name Printed